(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 195 36 206 A 1**

(51) Int. Cl.[6]: G 06 K 19/073

(21) Aktenzeichen: 195 36 206.3
(22) Anmeldetag: 28. 9. 95
(43) Offenlegungstag: 4. 4. 96

DE 195 36 206 A 1

(30) Unionspriorität: (32) (33) (31)
30.09.94 KR 25043/94

(71) Anmelder:
Samsung Electronics Co. Ltd., Kyungki-Do, KR

(74) Vertreter:
Grünecker, Kinkeldey, Stockmair & Schwanhäusser, Anwaltssozietät, 80538 München

(72) Erfinder:
Kim, Jong-Chul, Suwon, KR; Hwang, Sung-Man, Eunpyeong, KR

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Intelligente Karte

(57) Ein Datenspeicher ist in n Blöcke aufgeteilt. Ein Statuswert zeigt an, ob in einem Vorspann des jeweiligen Blocks des Datenspeichers ein Kennwort vorhanden ist, wobei das Kennwort in einem Kennwortaufzeichnungsbereich aufgezeichnet ist. Auf die Speicherinformation des Datenspeichers kann zugegriffen werden, wenn das im aufgeteilten Datenspeicherbereich aufgezeichnete Kennwort mit einem von außen empfangenen Kennwort übereinstimmt.

DE 195 36 206 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 02. 96 602 014/506

Beschreibung

Die vorliegende Erfindung bezieht sich auf ein Verfahren zum Schutz von Information auf einer intelligenten Karte und insbesondere auf eine solche intelligente Karte, bei der über einen Kennwortvergleichsvorgang auf einen Datenspeicherbereich zugegriffen wird.

Im allgemeinen werden ein IC-Karten (Karten mit integriertem Schaltkreis) klassifiziert in Speicherkarten, die Nur-Lese-Datenspeicher sind, und in intelligente Karten zum Lesen und Schreiben von Daten. Zwischen der Speicherkarte und der intelligenten Karte besteht ein großer Unterschied, indem die erstere nur eine Speichervorrichtung zum Speichern fester Informationen besitzt, während die letztere zusätzlich zur Speichervorrichtung eine Zentraleinheit (CPU) aufweist. Die CPU der intelligenten Karte führt aufgrund eines von einem externen Kartenleser gegebenen Steuersignals einen Zugriff (Lesen/Schreiben) auf die Speichervorrichtung aus und bewerkstelligt über eine serielle Eingabe/Ausgabe- (SIO)-Vorrichtung den Datenaustausch mit dem externen Kartenleser gemäß dem ISO-7816-Protokoll, so daß sehr einfach Information innerhalb der Speichervorrichtung korrigiert oder hinzugefügt werden kann.

Seit kurzem zeigen die IC-Karten aufgrund der Möglichkeiten für den Herausgeber, den Aussteller sowie den Halter und aufgrund der hohen Zuverlässigkeit hinsichtlich der Sicherheit der privaten Information eine zunehmende Tendenz in Richtung der Verwendung der intelligenten Karte.

Fig. 2 zeigt den schematischen Innenaufbau einer intelligenten Karte, die im Stand der Technik weit verbreitet ist. Eine CPU **103** führt aufgrund eines von außen gegebenen Steuersignals über eine SIO **101** einen asynchronen Datenaustausch mit dem Kartenleser durch. Die CPU **103** greift auf einen elektrisch löschbaren und programmierbaren Nur-Lese-Speicher (EEPROM) **107** zu, der als Datenspeicher verwendet wird, um die Daten zur SIO **101** zu übertragen, und korrigiert oder ersetzt die Daten des EEPROM **107** oder fügt dem EEPROM **107** neue Daten hinzu, in Abhängigkeit von den von der SIO **101** übertragenen Daten.

Ein Nur-Lese-Speicher (ROM) **105**, d. h. eine Programmspeichervorrichtung, speichert ein Steuerprogramm, das zur Datenübertragung über die SIO **101** verwendet wird, sowie Betriebssystemdaten für den Zugriff auf den EEPROM **107**. Der EEPROM **107** speichert Information über den Halter, Herausgeber, Aussteller etc. Auf die im EEPROM **107** gespeicherte Information kann nicht immer von jedermann oder von irgendeinem Kartenleser zugegriffen werden, jedoch kann darauf zugegriffen werden, wenn eine zugeteilte Geheimnummer oder ein Kennwort übereinstimmt. Daher vergleicht die CPU **103** die über die SIO **101** übertragenen Daten mit einem im ROM **105** gespeicherten Kennwort und greift auf den EEPROM zu, wenn diese übereinstimmen. In einem solchen Fall kann die CPU **103** die vom Herausgeber, Aussteller oder Halter benötigten Daten ausgeben, korrigieren oder ergänzen, indem sie auf den EEPROM **107** zugreift. Wenn das vom Halter angegebene Kennwort nicht mit dem bei der Initialisierung gespeicherten Kennwort übereinstimmt, kann nicht auf den EEPROM **107** zugegriffen werden, so daß es unmöglich ist, die Information zu lesen, zu korrigieren oder zu ergänzen.

Bei der herkömmlichen intelligenten Karte wird von der Software überprüft, ob das vom Halter angegebene Kennwort mit dem bei der Initialisierung gespeicherten

Kennwort übereinstimmt oder nicht. Durch diese Vorgehensweise nimmt die Belastung der CPU zu. Da ferner einfach auf die Informationen des Datenspeichers und auf für den Halter unnötige Information zugegriffen werden kann, wird die Sicherheit für die Wahrung eines Geheimnisses des Halters verringert, wobei die Information mißbraucht werden kann.

Es ist daher eine Aufgabe der vorliegenden Erfindung, eine intelligente Karte zu schaffen, die die Zuverlässigkeit der Informationshandhabung eines Datenspeichers erhöht, indem der Datenspeicher in Blöcke aufgeteilt wird, in jedem Block ein Kennwort registriert wird und auf die Information eines jeweiligen Bereichs über einen Kennwortvergleichsvorgang zugegriffen wird.

Es ist eine weitere Aufgabe der vorliegenden Erfindung, eine intelligente Karte zu schaffen, die die Belastung einer CPU verringert und eine für den Kennwortvergleich erforderliche Zeitspanne verkürzt.

Es ist eine weitere Aufgabe der vorliegenden Erfindung, eine intelligente Karte zu schaffen, die als eine Karte mit verschiedenen Speichervorrichtungen verwendet werden kann, indem ein Datenspeicher in verschiedene Bereiche aufgeteilt wird.

Diese Aufgaben werden erfindungsgemäß gelöst durch eine intelligente Karte und ein Zugriffsverfahren, die die in den unabhängigen Ansprüchen 1, 2, 5 und 8 angegebenen Merkmale besitzen. Die abhängigen Ansprüche sind auf bevorzugte Ausführungsformen gerichtet.

Gemäß einem Aspekt der vorliegenden Erfindung kann eine CPU nur über einen Kennwortvergleichsvorgang, der in einem Informationsschutzprozessor implementiert ist, auf einen Datenspeicher zugreifen. Der Informationsschutzprozessor umfaßt: eine Speicheraufteilungs- und Kennwortdatenempfangsschaltung zum Erzeugen eines Zuweisungssignals, die auf einen Kennwortspeicherbereich des jeweiligen Blocks zugreift und ein von außen empfangenes Kennwort empfängt; eine Kennwortvergleichsschaltung zum Vergleichen des von der Speicheraufteilungs- und Kennwortdatenempfangsschaltung erzeugten Kennwortes mit dem im Datenspeicher gespeicherten Kennwort; eine Zugriffsteuersignalerzeugungsschaltung zum Erzeugen eines Zugriffsteuersignals, die auf den Datenspeicher zugreift, wenn beide Kennwörter übereinstimmen; eine Kennwortaufzeichnungsbereichfestlegungsschaltung zum bevorzugten Zuweisen eines Kennwortaufzeichnungsbereiches, wenn ein bezeichneter Block des Datenspeichers ausgewählt ist, und zum Festlegen eines Informationsaufzeichnungsbereiches, auf den zugegriffen werden soll; eine Zugriffadressenerzeugungsschaltung zum Erzeugen eines Adreßsignals für den Kennwort- und Informationszugriff aus den Ausgaben der Speicheraufteilungs- und Kennwortdatenempfangsschaltung und der Kennwortaufzeichnungsbereichfestlegungsschaltung; und eine Zeitablaufsteuersignalerzeugungsschaltung zum Erzeugen eines Adreßsignals, die einen Block für den Zugriff auf den Datenspeicher zuweist und ein Zeitablaufsteuersignal für einen Kennwortvergleich erzeugt.

Weitere Aufgaben, Merkmale und Vorteile der vorliegenden Erfindung werden deutlich beim Lesen der folgenden Beschreibung bevorzugter Ausführungsformen, die auf die beigefügten Zeichnungen Bezug nimmt, in welchen ähnliche Bezugszeichen und Symbole verwendet werden, um ähnliche Elemente zu bezeichnen; es zeigen:

Fig. 1 ein Blockschaltbild, das den inneren Aufbau

einer intelligenten Karte gemäß der vorliegenden Erfindung zeigt;

Fig. 2 das bereits erwähnte Blockschaltbild, das den inneren Aufbau einer herkömmlichen intelligenten Karte zeigt;

Fig. 3A und 3B ein Beispiel der Aufteilung eines Datenspeichers in gleich große Blöcke und ein Beispiel für die Speicherung eines Kennwortes;

Fig. 4 ein Blockschaltbild, das den inneren Aufbau eines Informationsschutzprozessors der Fig. 1 zeigt;

Fig. 5 einen genauen Schaltplan der Fig. 4;

Fig. 6 einen genauen Schaltplan der in Fig. 5 gezeigten Zeitablaufsteuersignalerzeugungsschaltung;

Fig. 7 einen genauen Schaltplan der in Fig. 5 gezeigten Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung;

Fig. 8 ein Zeitablaufdiagramm für die Schaltung der Fig. 5, wenn kein Kennwort vorhanden ist;

Fig. 9 ein Zeitablaufdiagramm für die Schaltung der Fig. 5, wenn ein Kennwort vorhanden ist; und

Fig. 10 ein Zeitablaufdiagramm für die Schaltung der Fig. 5, wenn ein Kennwortvergleichsergebnis negativ ausfällt.

Wie in Fig. 1 gezeigt, ist der Datenspeicher gemäß der vorliegenden Erfindung ein EEPROM und ist in gleich große Blöcke aufgeteilt. Jeder abgeteilte Block ist in ein Kennwortstatusregister, einen Kennwortaufzeichnungsbereich sowie einen Informationsspeicherbereich unterteilt. Um in den jeweiligen Block ein Kennwort einzutragen, wird in einem MSB (höchstwertiges Bit) des Kennwortstatusregisters des jeweiligen Blocks eine "1" gesetzt, woraufhin das Kennwort in den Kennwortaufzeichnungsbereich eingetragen wird. Um den abgeteilten Datenspeicherbereich, dem das Kennwort zugewiesen ist, zu verwenden, wird geprüft, ob das Kennwort vorhanden ist oder nicht. Wenn im MSB des Kennwortstatusregisters eine "1" eingetragen ist, wird das im Kennwortaufzeichnungsbereich eingetragene Kennwort mit dem von der CPU 103 gegebenen Kennwort verglichen. Wenn diese gleich sind, trägt die CPU 103 in das dem MSB folgende Bit des Kennwortstatusregisters eine "1" ein, was anzeigt, daß auf den Informationsspeicherbereich dieses Block zugegriffen werden kann. Falls nicht, wird in das dem MSB folgende Bit des Kennwortstatusregisters eine "0" eingetragen, was anzeigt, daß auf den Informationsspeicherbereich nicht zugegriffen werden kann. Wenn das MSB des Kennwortstatusregisters "0" ist, bedeutet dies, daß kein Kennwort zugewiesen worden ist. In diesem Fall ist der zugehörige Speicherbereich ohne einen Kennwortvergleichsvorgang verfügbar, wobei dieser Zustand üblicherweise der Anfangszustand ist.

Wie in Fig. 1 gezeigt, umfaßt ein EEPROM 107 einen ROM-Bereich, der ein Programmbereich zum Speichern eines Betriebsprogramms ist, sowie einen EEPROM-Bereich, der ein Datenspeicherbereich zum Speichern von Informationsdaten ist, und weist verschiedenen Bereichen eine konstante Größe zu. Auf dem Datenspeicherbereich, der die Informationsdaten speichert, wird von der CPU 103 direkt oder über einen Informationsschutzprozessor 201 zugegriffen. Auf den Programmbereich wird von der CPU 103 direkt zugegriffen. Anfangs kann auf den Datenspeicherbereich einfach zugegriffen werden. Wenn jedoch einmal ein Kennwort registriert ist, wird auf den zugehörigen Datenspeicherbereich über einen Kennwortvergleichsvorgang für einen zu benutzenden Bereich zugegriffen.

Die Fig. 3A und 3B zeigen den Datenspeicher 301 und einen Kennwortaufzeichnungsbereich 303, der ein Schutzblockauswahlregister (PBSEL) 306 im höchstwertigen Byte des Kennworts (PSB) der jeweiligen aufgeteilten Bereiche BL_F bis BL_0 enthält. Der Datenspeicher 301 ist in N Bereiche aufgeteilt. Wenn jeder Bereich als "Block" bezeichnet wird, können die jeweiligen Blöcke die gleiche Größe oder verschiedene Größen besitzen. Die jeweiligen Blöcke BL_0 bis BL_F werden durch einen von der CPU 103 gegebenen Wert gesteuert. Die CPU 103 bestimmt eine Änderung eines Statuswerts des PBSEL 306 aus dem PSB.

Wie in Fig. 3 gezeigt, ist der Datenspeicher 301 in 16 Blöcke aufgeteilt, wobei das PBSEL 306 vier Bits umfaßt. Da mit vier Bits 16 verschiedene Werte erzeugt werden können, kann jeder Vier-Bit-Wert für jeweils einen Block verwendet werden. Wenn jede Einheitsblockgröße 0,5 kBytes beträgt, beträgt die Kapazität des Datenspeichers 301 8 kBytes. Wenn die vier Bits des PBSEL 306 den Wert "0000B" aufweisen, ist ein erster Block BL_0 von 0,5 kBytes ausgewählt, während ein sechster Block BL_4 von 0,5 kBytes ausgewählt ist, wenn sie einen Wert von "0101B" aufweisen. Vier höherwertige Bits des PSB werden verwendet, um den Block des PBSEL 306 auszuwählen, während die anderen Bits als Adresse für den Datenspeicher 301 verwendet werden. Um z. B. auf eine Adresse 20H des sechsten Blocks BL_4 zuzugreifen, müssen die entsprechenden Bits des PBSEL 306 auf den Wert "0101B" gesetzt sein, wobei die Adresse für den Datenspeicher 301 auf den Wert "0020H" gesetzt sein muß. Die Adresse 20H des sechsten Blocks BL_4 wird in der Adresse des Datenspeichers 301 als Adresse 520H verarbeitet. Dieser Vorgang hängt davon ab, welcher Wert in das PBSEL eines Speicherblockauswahlregisters einer Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 im Informationsschutzprozessor 201 geschrieben ist.

Fig. 4 zeigt den in Fig. 1 gezeigten Informationsschutzprozessor 201. Eine Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 decodiert Datenblockauswahl- und Kennwortempfangsadreßauswahlsignale, die von der CPU 103 erzeugt werden, um Daten für die Auswahl des aufgeteilten Blocks und den Kennwortaufzeichnungsbereich zu erzeugen, und zeichnet Kennwortdaten auf, die von außen empfangen werden, um für den Zeitpunkt des Vergleichens die Kennwortdaten zu erzeugen. Die CPU 103 legt an die Speicherblockauswahlsignalerzeugungs- und Kennwortempfangsschaltung 407 ein Lesesteuersignal an, um einen Datenspeicherzugriff-Zustand oder einen Kennwortvergleichsvorgang-Zustand zu überprüfen.

Ein erster Kennwortkomparator 419 vergleicht bitweise die Kennwortdaten, die von der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 erzeugt werden, mit dem im ausgewählten Block des Datenspeichers aufgezeichneten Kennwort, um ein Kennwortvergleichsergebnis für ein Byte zu erzeugen. Eine Kennwortzwischenspeicherschaltung 409 speichert vorübergehend das Kennwortvergleichsergebnis, bis alle Bytes des Kennwortes verglichen worden sind. Ein zweiter Kennwortkomparator 421 bestätigt das Kennwortvergleichsergebnis für alle in der Kennwortzwischenspeicherschaltung 409 gespeicherten Bytes vor einem Vergleichsabschlußzeitpunkt, der von einer Zeitablaufsteuersignalerzeugungsschaltung 405 erzeugt wird. Eine Zugriffsteuersignalerzeugungsschaltung 403 erzeugt ein Zugriffsteuersignal, das anzeigt, daß auf den ausgewählten Datenspeicherbe-

reich zugegriffen werden kann, wenn das Kennwortvergleichsergebnis, das vom zweiten Kennwortkomparator 421 erzeugt worden ist, übereinstimmt und eine Information vorliegt, daß für den ausgewählten Datenspeicherbereich ein Kennwort vorhanden ist.

Die Zeitsteuersignalerzeugungsschaltung 405 zählt einen Takt in Abhängigkeit von einem Startsignal, das gleichzeitig mit der Blockzuweisungsdecodierung der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 erzeugt wird, um ein Decodierungssignal zum Lesen eines Kennwortvergleichszyklus, ein Vergleichstaktsignal und das in der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 aufgezeichnete Kennwort zu erzeugen, und übergibt an den zweiten Kennwortkomparator 421 ein Kennwortvergleichabschluß-Steuersignal. Eine Kennwortspeicherbereichfestlegungsschaltung 415 erzeugt eine Adresse, um vorzugsweise den Kennwortspeicherbereich des jeweiligen Blocks des Datenspeichers zuzuweisen. Eine Zugriffadreßsignalerzeugungsschaltung 413 wählt einen Block des in N Blöcke unterteilten Datenspeichers mittels eines Signals aus, das von der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 erzeugt worden ist, erzeugt ein Adreßsignal für die Zuweisung eines Kennwortzugriffsignals und ein Adreßsignal für den Zugriff auf einen Informationsspeicherwert, wenn der Kennwortvergleich abgeschlossen ist.

Fig. 5 ist ein genaueres Schaltbild der Schaltung von Fig. 4. Die Leitungen 1502 und 1503, die mit der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 und mit der Zeitsteuersignalerzeugungsschaltung 405 verbunden sind, werden von einem Datenbus, einem Adreßbus und einem Steuerbus zwischen der CPU 103 und dem EEPROM 107 mitbenutzt, wobei jeweils Steuersignale, Adressen und Daten über diese empfangen werden. Die Leitung 502 [a(7 : 0), RESET, CLK, NREG RD, NREG WR] ist eine Eingangsleitung der CPU 103. Die im EEPROM 107 gespeicherten Kennwortdaten werden über die Leitung 503 [ad(7 : 0)] empfangen. Ein Freigabesteuersignal ECE des EEPROMs 107, der mit der Zeitablaufsteuersignalerzeugungsschaltung 405 verbunden ist, greift auf den EEPROM 107 zu, wenn ein Zugriffsteuersignalzugriff während eines Kennwortvergleichszyklus COMPCYCLE stattfindet. Der Verarbeitungszustand des Informationsschutzprozessors 201 wird über einen Datenbus idb(7 : 0), der mit der Speicherblockauswahlsignal erzeugungs- und Kennwortdatenempfangsschaltung 407 verbunden ist, von der CPU 103 überprüft.

Eine Rücksetzsignalleitung der CPU 103 ist mit einem Rücksetzanschluß R eines Flipflops 571 der Zugriffsteuersignalerzeugungsschaltung 403 und mit jedem Rücksetzanschluß der Zeitablaufsteuersignalerzeugungsschaltung 405 und der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 sowie ferner über ein NICHT-ODER-Gatter 525 der Kennwortzwischenspeicherschaltung 409 mit jedem Rücksetzanschluß R der Flipflops 577 bis 587 verbunden. Ein Taktsignal clk der CPU 103 liegt als Grundbetriebstakt an der Zeitablaufsteuersignalerzeugungsschaltung 405 und der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 an. Ein Registerschreibsteuersignal nreg wr, das mit der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 verbunden ist, schreibt die Kennwortdaten in den abgeteilten Block des Datenspeichers. Ein Registerlesesteuersignal nreg rd, das mit der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 verbunden ist, liest über den Datenbus idb von der CPU 103 ein Informationsschutzstatussignal.

Ein Treiberstartsteuersignal START der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 liegt an der Zeitablaufsteuersignalerzeugungsschaltung 405, der Zugriffsteuersignalerzeugungsschaltung 403 und der Kennwortzwischenspeicherschaltung 409 an und wählt über den Adreßbus a(7 : 0) mittels eines Speicherblockzuweisungsadreßsignals den Block aus, wenn das Registerschreibsteuersignal nreg wr anliegt. Wenn im EEPROM 107 kein Kennwort gespeichert ist, kann ein Kennwort aufgezeichnet werden, während dann, wenn ein Kennwort vorhanden ist, ein Kennwortvergleich eingeleitet wird. Ein Speicherblockzuweisungsadreßsignal PBSR der Speicherblockauswahlsignal erzeugungs- und Kennwortdatenempfangsschaltung 407 ist mit einem Multiplexer 575 der Zugriffadreßsignalerzeugungsschaltung 413, NICHT-ODER-Gattern 507, 509 sowie einem Invertierer 541 der Kennwortspeicherbereichfestlegungsschaltung 415 verbunden und bezeichnet eine Position für das Auswählen des abgeteilten Blocks des Datenspeichers und für das Zugreifen auf das Kennwort des jeweiligen Blocks.

Ein Kennwortvergleichszyklussignal COMPCYCLE der Zeitablaufsteuersignalerzeugungsschaltung 405 wird als ein Zeitablaufsignal verwendet, das ein Kennwortvergleichsintervall angibt, und ist mit einem UND-Gatter 555 der Zugriffadreßsignalerzeugungsschaltung 413 und einem Invertierer 537 der Kennwortspeicherbereichsfestlegungsschaltung 415 verbunden. Während des Kennwortvergleichszyklus werden die Kennwortdaten aus dem Speicherbereich des EEPROM 107 gelesen und verglichen. Ferner ist das Kennwortvergleichszyklussignal compcycle der Zeitablaufsteuersignalerzeugungsschaltung 405 mit dem Kennwortvergleichszyklussignal compcycle der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 verbunden. Während des Kennwortvergleichszyklus wird ein Block für den Informationszugriff des EEPROMs 107 bezeichnet, der Kennwortaufzeichnungsbereich bezeichnet und die Kennwortdaten für einen Vergleich erzeugt.

Ein Adreßsignal add(2 : 0) der Zeitablaufsteuersignalerzeugungsschaltung 405 ist mit der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 verbunden und wird als Registerfreigabe-Auswahldecodierungssignal zum sequentiellen Einlesen des Kennwortes in ein internes Register verwendet. Ein Kennwortvergleichstaktsignal COMPCLK ist mit jedem Taktanschluß C der Flipflops 579 bis 587 der Kennwortzwischenspeicherschaltung 409 verbunden und wird als Takt zum Zwischenspeichern eines Kennwortvergleichsergebnisses verwendet. Ein Kennwortvergleichsabschlußsignal ENDCOMP, das den Abschluß eines Kennwortvergleichs anzeigt, ist mit dem zweiten Kennwortkomparator 421 verbunden. Ein MSB-Anzeigesignal PASSW-7, das anzeigt, ob ein Kennwort vorhanden ist, ist mit einem NICHT-ODER-Gatter 545 der Zugriffsteuersignalerzeugungsschaltung 403 verbunden und dient dazu, daß nur auf einen Block mit Kennwort zugegriffen werden kann.

Die Zeitablaufsteuersignalerzeugungsschaltung 405 ist in Fig. 6 genauer gezeigt. Die Flipflops 641 bis 653 werden durch das Rücksetzsignal RESET initialisiert.

Das Flipflop 641 wird durch das Startsignal START gesetzt, wobei ein Ausgangsanschluß Q des Flipflops 641 eine logische 1 erzeugt, wodurch das Flipflop 643 gesetzt wird. Das Taktsignal CLK ist über einen Invertierer 629 und ein UND-Gatter 606 mit einem Taktanschluß C des Flipflops 643 verbunden. Indem der Ausgang des Flipflops 641 mittels der Flipflops 643 bis 651 geteilt wird, wird das Kennwortvergleichszyklussignal COMPCYCLE erzeugt. Der Ausgang des Flipflops 651 und der Ausgang des Flipflops 653 liegen am UND-Gatter 605 an. In Abhängigkeit vom Ausgang des UND-Gatters 605 und des Kennwortdurchgangssignals PASSWDPASS wird von einem NICHT-ODER-Gatter 617 das Kennwortvergleichsabschlußsignal ENDCOMP erzeugt. Das Vergleichstaktsignal COMPCLK wird von den Ausgängen der Flipflops 643 und 653 erzeugt. Ein Multiplexer 655 wählt in Abhängigkeit vom Kennwortvergleichszyklussignal COMPCYCLE einen Eingangsanschluß A oder B aus. Wenn das Kennwortvergleichszyklussignal COMPCYCLE gleich logisch 1 ist, werden die Ausgänge der Flipflops 645, 647 und 649 ausgewählt, um das Adreßsignal add(2 : 0) für die Zuweisung einer Kennwortspeicherposition zu erzeugen, während dann, wenn es gleich logisch 0 ist, das Adreßsignal a(2 : 0) für den Zugriff der CPU 103 erzeugt wird.

Der Eingangsanschluß A des Multiplexers 655, das Taktsignal CLK sowie der Ausgang des Flipflops 643 liegen an einem NICHT-UND-Gatter 621 an, welches das MSB-Anzeigesignal PASSW-7 für die Kennwortdaten erzeugt. Ein NICHT-ODER-Gatter 615 erzeugt das Kennwortvergleichszyklussignal COMPCYCLE und das Zugriffssteuersignal ACCESS der Zugriffsteuersignalerzeugungsschaltung 403, um das Freigabesteuersignal ECE für den Zugriff auf das EEPROM 107 zu erzeugen.

Fig. 7 zeigt die in Fig. 5 gezeigte Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407. Das Rücksetzsignal RESET initialisiert ein Speicherblockzuweisungsregister 759, das eine Adresse für die Zuweisung eines Speicherblocks für den Kennwortzugriff speichert. Ein Speicherblockzuweisungsdecodierer 741 und die Kennwortregisterauswahldecodierer 742 bis 752 werden durch das Registerschreibsteuersignal NREG WR, das von der CPU 103 erzeugt wird, in einen Schreibmodus versetzt. Das von der CPU 103 erzeugte Adreßsignal a(7 : 0) ist über einen Invertierer 703 mit dem Speicherblockzuweisungsdecodierer 43 und mit den Kennwortregisterauswahldecodierern 742 bis 752 verbunden. Ferner ist das Adreßsignal a(7 : 0) über ein NICHT-ODER-Gatter 725 und einen Invertierer 705 mit dem Speicherblockzuweisungsdecodierer 741 und mit den Kennwortregisterauswahldecodierern 742 bis 753 verbunden. Die Anzahl der Kennwortregisterauswahldecodierer 742 bis 752 entspricht der Anzahl der Kennwörter.

Die Dreistufenpuffer 727 und 729 schalten das Zugriffsteuersignal ACCESS bzw. das Kennwortvergleichszyklussignal COMPCYCLE in Abhängigkeit von einem Ausgangssignal ad des Speicherblockzuweisungsdecodierer 741 durch, der Eingangssignale decodiert. Ein Schreibsteuerausgangssignal NREG WR des Speicherblockzuweisungsdecodierer 741 ist das Startsignal START der Zeitablaufsteuersignalerzeugungsschaltung 405 und der Zugriffsteuersignalerzeugungsschaltung 403 und gibt das Speicherblockzuweisungsregister 759 zum Schreiben frei. In einem solchen Fall werden die Daten für die Zuweisung des Speicherblocks auf dem Datenbus idb(7 : 0), die die CPU 103 von der SIO 101 empfängt, im Speicherblockzuweisungsregister 759 aufgezeichnet. Das Speicherblockzuweisungsregister 759 erzeugt das Blockzuweisungsadreßsignal pbsr(3 : 0). Wenn die Kennwortregisterauswahldecodierer 742 bis 752 sequentiell durch die Eingangssignale über den Adreßbus a(7 : 0) decodiert werden, werden die entsprechenden Kennwortaufzeichnungsregister 761 bis 773 zum Schreiben freigegeben. Dann werden die Kennwortdaten auf dem Datenbus idb(7 : 0), die die CPU 103 über die SIO 101 empfängt, nacheinander in den Kennwortaufzeichnungsregistern 761 bis 773 abgelegt.

Damit die CPU 103 den Betriebszustand des Informationsschutzprozessors 201 überprüft, wenn das Lesesteuersignal NREG RD anliegt, wird der Ausgang eines Flipflops 755 von einem Flipflop 704 zwischengespeichert, um einen Bustreiber 702 freizugeben. Die Ausgänge der Dreistufenpuffer 727 und 729 einer Informationsschutzprozessorzustandssignal-Erzeugungsschaltung 720 werden auf den Datenbus idb übertragen, der über den Bustreiber 702 mit der CPU 103 verbunden ist. Anschließend kann die CPU 103 den Betriebszustand des Informationsschutzprozessors 201 überprüfen. Die NICHT-UND-Gatter 775 bis 787 decodieren das Kennwortvergleichszyklussignal COMPCYCLE und das Kennwortaufzeichnungsbereichzuweisungsadreßsignal ad(2 : 0) der Zeitablaufsteuersignalerzeugungsschaltung 405. Die Ausgänge der NICHT-UND-Gatter 775 bis 787 werden von den Invertierern 709 bis 721 invertiert und an jeden Ausgangsfreigabeanschluß r der Kennwortaufzeichnungsregister 761 bis 771 angelegt, um nacheinander die aufgezeichneten Kennwortdaten auszulesen. Die von der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 erzeugten Kennwortdaten werden an ein Exklusiv-ODER-Gatter 523 des ersten Kennwortkomparators 419 angelegt. Das Exklusiv-ODER-Gatter 523 empfängt ferner über den Datenbus ad(7 : 0) die vom EEPROM 107 erzeugten Kennwortdaten. Das Exklusiv-ODER-Gatter 523 legt ein Kennwortvergleichsergebnis für ein Byte an ein NICHT-UND-Gatter 502 an. Der Ausgang des ersten Kennwortkomparators wird in einem der Flipflops 577 bis 589 der Kennwortzwischenspeicherschaltung 409 zwischengespeichert. Die Vergleichsergebnisse für sieben Bytes werden an ein UND-Gatter 505 des zweiten Kennwortkomparators 421 angelegt. Wenn alle Ausgänge des UND-Gatters 505 gleich logisch 1 sind, ist das Kennwortvergleichsergebnis positiv, während es negativ ist, falls dies nicht zutrifft. Der Ausgang des zweiten Kennwortkomparators 421 liegt zusammen mit dem Ausgangssignal des NICHT-ODER-Gatters 545, das das MSB-Anzeigesignal PASSW-7 empfängt, am ODER-Gatter 547 der Zugriffssignalerzeugungsschaltung 403 an. Das ODER-Gatter 547 erzeugt ein Kennwortdurchgangssteuersignal PASSWDPASS, das anzeigt, daß das Kennwort akzeptiert worden ist. Der Ausgang des ODER-Gatters 547 und der Ausgang des Flipflops 571 liegen am NICHT-UND-Gatter 503 an. Ein Flipflop 573, das die Ausgabe des NICHT-UND-Gatters 503 empfängt, erzeugt das Zugriffsteuersignal access, das anzeigt, daß auf einen zugehörigen Block zugegriffen werden kann. Das Zugriffsteuersignal access liegt an der Zeitablaufsteuersignalerzeugungsschaltung 405 und der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 an. Somit greift die CPU 103 auf den Informationsspeicherbereich zu, indem sie den EEPROM 107 mittels des Zugriffsteuersignals access, das an der Zeitablaufsteuersignalerzeu-

gungsschaltung 405 anliegt, über das in Fig. 6 gezeigte NICHT-ODER-Gatter 615 freigibt. Da ferner das Zugriffsteuersignal access an der Informationsschutzprozessorzustanderzeugungsschaltung 720 der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 anliegt, befindet sich die CPU 103 in einem zugriffsfähigen Zustand.

Im folgenden wird ein Initialisierungsmodus oder Kein-Kennwort-Modus beschrieben. In einem Kein-Kennwort-Modus, d. h., wenn sich ein Chip im Initialisierungszustand befindet oder im Datenspeicherbereich des EEPROMs 107 kein Kennwort vorhanden ist, kann auf den Datenspeicherbereich immer zugegriffen werden. Im folgenden wird mit Bezug auf Fig. 8 der Kein-Kennwort-Modus beschrieben.

Wenn das in (8a) der Fig. 8 gezeigte Taktsignal CLK an den Speicherblockzuweisungsdecodierer 741 und die Kennwortregisterdecodierer 742 bis 752 der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 angelegt wird und das Registerschreibsteuersignal NREG WR auf logisch 0 zurückgenommen wird, wie in (8h) der Fig. 8 gezeigt ist, wird ein Adreßsignal des Adreßbusses a(7 : 0) direkt, über einen Invertierer 703 und über das NICHT-ODER-Gatter 725 und den Invertierer 705 an den Speicherblockzuweisungsdecodierer 741 und die Kennwortregisterauswahldecodierer 742 bis 752 angelegt, um das Speicherblockzuweisungsregister 759 und die Kennwortaufzeichnungsregister 761 bis 773 auszuwählen.

Wenn wie in (8f) der Fig. 8 gezeigt die Daten der gemeinsamen Eingangsanschlüsse ra0 bis ra3 des Speicherblockzuweisungsdecodierers 741 und der Kennwortregisterauswahldecodierer 742 bis 752 gleich "07H" sind, wird der Schreibsteueranschluß wr, der der Ausgang des Speicherblockzuweisungsdecodierers 741 zum Zuweisen des Speicherblocks ist, auf eine logische 1 geschaltet, um das Speicherblockzuweisungsregister 759 freizugeben und gleichzeitig das Startsignal START auf eine logische 1 zu setzen, wie in (8z) der Fig. 8 gezeigt ist. Das Startsignal START mit der logischen 1 liegt an der Zeitablaufsteuersignalerzeugungsschaltung 405 und der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 an. Da anfangs im EEPROM 107 kein Kennwort gesetzt ist, erzeugt das ODER-Gatter 547 der Steuersignalerzeugungsschaltung 403 eine logische 1, wie in (8g) der Fig. 8 gezeigt ist. Das Flipflop 641 der Zeitablaufsteuersignalerzeugungsschaltung 405 der Fig. 6 wird durch das Startsignal START mit der logischen 1 gesetzt, wie in (8z) der Fig. 8 gezeigt ist, wobei der Ausgangsanschluß Q desselben eine logische 1 erzeugt. Somit werden die Flipflops 643 und 651 gesetzt, um über ihre jeweiligen Ausgangsanschlüsse Q eine logische 1 zu erzeugen, während die Flipflops 645, 647 und 649 zurückgesetzt werden. Obwohl das Kennwortvergleichszyklussignal COMPCYCLE gleich logisch 1 ist, wird dann, wenn kein Kennwort vorhanden ist, das Kennwortvergleichszyklussignal COMPCYCLE vom Ausgang PASSWDPASS des ODER-Gatters 547 beeinflußt, wie in (8g) der Fig. 8 gezeigt ist. Somit ist das Kennwortvergleichszyklussignal COMPCYCLE gleich logisch 1, während das Startsignal START gleich logisch 1 ist, wie in (8z) der Fig. 8 gezeigt ist. Während das Kennwortvergleichszyklussignal COMPCYCLE gleich logisch 1 ist, sind die Daten add(2 : 0) des Ausgangsanschlusses A des Multiplexers 655 ausgewählt und liegen an den NICHT-UND-Gattern 775 bis 787 der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 der Fig. 7 an. Wenn der Ausgang des Invertierers 709 gleich logisch 1 ist, wird ein Wert des Speicherblockzuweisungsregisters 759 gelesen und das Speicherblockzuweisungsadreßsignal PBSR erzeugt, wie in (8t) der Fig. 8 gezeigt.

Das Speicherblockzuweisungssignal PBSR liegt am Multiplexer 575 der Zuweisungsadreßsignalerzeugungsschaltung 413 und an den NICHT-ODER-Gattern 507 und 509 sowie am Invertierer 541 der Kennwortspeicherbereicheinstellschaltung 415 an. Ein Signal des Datenbusses a(2 : 0) der CPU 103 liegt am Invertierer 539 und an den NICHT-ODER-Gattern 517 und 521 an. Das NICHT-ODER-Gatter 519 empfängt die Ausgaben der NICHT-ODER-Gatter 517 und 521. Das NICHT-ODER-Gatter 513 empfängt die Ausgaben der NICHT-ODER-Gatter 511 und 519. Der Ausgang des NICHT-UND-Gatters 563, das die Ausgabe des NICHT-ODER-Gatters 513 empfängt, liegt an den Auswahlanschlüssen des Multiplexers 575 an. Der Multiplexer 575 erzeugt das Blockzuweisungssignal PBSR der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407. Ein UND-Gatter 555 erzeugt durch die Ausgabe des NICHT-ODER-Gatters 507 während des Kennwortvergleichszyklus, der von der Zeitablaufsteuersignalerzeugungsschaltung 405 erzeugt wird, eine logische 1, während die UND-Gatter 557, 559 und 561 eine logische 0 erzeugen. Da sich ein Adreßwert in Abhängigkeit mit der Ausgabe eines ODER-Gatters 553 verändert, wird die Kennwortspeicherposition eines ausgewählten Blocks automatisch festgelegt. Die Kennwortaufzeichnungsregister 761 bis 773 werden freigegeben, indem nacheinander die Kennwortregisterauswahldecodierer 742 bis 752 decodiert werden, wobei die über die SIO 101 empfangenen Kennwortdaten nacheinander in den Kennwortaufzeichnungsregistern 761 bis 763 abgelegt werden. Wenn im EEPROM 107 kein Kennwort vorhanden ist, wird das Eingangssignal ad(7 : 0) des NICHT-ODER-Gatters 545 auf logisch 0 gesetzt.

Wenn die MSB-Zuweisungsadresse PASSW-7 der Zeitablaufsteuersignalerzeugungsschaltung 405 gleich logisch 0 ist, erzeugt das NICHT-ODER-Gatter 545 eine logische 1. Das ODER-Gatter 547 erzeugt ungeachtet der Ausgabe des zweiten Kennwortkomparators 505 eine logische 1. Das Flipflop 571 wird durch das Startsignal START mit einer logischen 1 gesetzt und erzeugt über den Ausgangsanschluß Q eine logische 1. Somit erzeugt das NICHT-UND-Gatter 503 eine logische 0. Das Flipflop 573 erzeugt eine logische 0, wie in (8w) der Fig. 8 gezeigt ist. Das Zugriffsteuersignal ACCESS mit der logischen 0 liegt am NICHT-ODER-Gatter 615 der Zeitablaufsteuersignalerzeugungsschaltung 405 an, um das EEPROM 107 zu sperren und liegt ferner am Dreistufenpuffer 727 der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 an, um 702 durch die Ausgabe eines Informationsschutzverarbeitung-Überprüfungsdecodierers 750 den Bustreiber 702 freizugeben. Die CPU 103 liest die Ausgabe der Informationsschutzverarbeitungszustandsignal-Erzeugungsschaltung 720 aus, um den Betriebszustand zu überprüfen.

Wenn im EEPROM 107 kein Kennwort vorhanden ist, kann somit von der CPU 103 auf den Datenspeicherbereich zugegriffen werden. Die Information wird gespeichert, indem jedem Block ein Kennwort zugewiesen wird. Nach dem Setzen einer "1" im Kennwortzustandsregister ist das gewünschte Kennwort festgelegt.

Im folgenden wird der Kennwortvergleichsmodus beschrieben. Wenn im Datenspeicherbereich des

EEPROMs 107 das Kennwort festgelegt ist und ein Vergleichsergebnis mit dem von außen empfangenen Kennwort positiv ausfällt, kann in einem Kennwortmodus auf die Information des Datenspeicherbereichs zugegriffen werden. Wenn im EEPROM 107 ein Kennwort festgelegt ist, ist der Eingangsanschluß 546 des NICHT-ODER-Gatters 545 gleich logisch 1. Wenn das Kennwortschreibsteuersignal NREG WR auf logisch 0 umgeschaltet wird, wie in (9h) der Fig. 9 gezeigt ist, werden die Speicherblockzuweisungsdecodierer 741 und die Kennwortregisterauswahldecodierer 742 bis 752 der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 in einen Schreibfreigabemodus versetzt. Der Speicherblockzuweisungsdecodierer 741 erzeugt aufgrund des über den Adreßbus a(7 : 0) der CPU 103 empfangenen Adreßsignals das Startsignal START, wie in (9z) der Fig. 9 gezeigt ist, und gibt gleichzeitig das Speicherblockzuweisungsregister 759 frei, wodurch Blockzuweisungsdaten, die über die SIO 101 übertragen werden, aufgezeichnet werden.

Die Dreistufenpuffer 727 und 729 der Informationsschutzverarbeitungszustandssignal-Erzeugungsschaltung 720 schalten das Zugriffsteuersignal ACCESS und das Kennwortvergleichszyklussignal COMPCYCLE durch. Wenn das in (9z) der Fig. 9 gezeigte Startsignal START an die Zeitablaufsteuersignalerzeugungsschaltung 405 angelegt wird, erzeugt das Flipflop 641 am Ausgangsanschluß Q eine logische 1. Die Flipflops 645, 647 und 649 werden zurückgesetzt und erzeugen an ihren Ausgangsanschlüssen Q eine logische 0. Das Taktsignal CLK in (9a) der Fig. 9 wird in einem Invertierer 629 invertiert und setzt über das UND-Gatter 606 die Flipflops 643 und 651. Die Flipflops 643 und 651 erzeugen an ihren Ausgangsanschlüssen Q eine logische 1. Somit wird das Kennwortvergleichszyklussignal COMPCYCLE auf eine logische 1 gesetzt, wie in (9p) der Fig. 9 gezeigt ist, wobei das NICHT-ODER-Gatter 615 eine logische 0 erzeugt, wie in (9k) der Fig. 9 gezeigt ist, um durch Freigeben des EEPROMs 107 die Kennwortdaten aus zulesen.

Der Ausgang des Flipflops 651 wird auf einer logischen 1 eines konstanten Kennwortvergleichszyklussignals COMPCYCLE, das in (9p) der Fig. 9 gezeigt ist, gehalten, indem der Takt auf den Anschlüssen C der Flipflops 643 bis 651 gezählt wird. Das Kennwortvergleichstaktsignal COMPCLK, das in (9x) der Fig. 9 gezeigt ist, liegt an den Taktanschlüssen C der Flipflops 579 bis 587 der Kennwortzwischenspeicherschaltung 409 an. Während der logischen 1 des Kennwortvergleichszyklussignals COMPCYCLE wählt der Multiplexer 655 Daten aus, die von den Zählanschlüssen der Flipflops 643 bis 651 erzeugt werden, um diese an den Invertierer 707 und die NICHT-UND-Gatter 775 bis 787 anzulegen. Das NICHT-UND-Gatter 621 erzeugt aufgrund der Ausgaben der Flipflops und des Taktsignals CLK das MSB-Anzeigesignal PASSW-7.

Der im Speicherblockzuweisungsregister 759 gespeicherte Blockzuweisungswert kann von der CPU 103 über den Bustreiber 702 gelesen werden und wird an den Multiplexer 575 der Zugriffadreßsignalerzeugungsschaltung 413, die NICHT-ODER-Gatter 507, 509 und den Invertierer 541 der Kennwortspeicherbereichfestlegungsschaltung 415 angelegt. Das UND-Gatter 563 erzeugt aufgrund der Ausgaben der NICHT-ODER-Gatter 517, 521 eine logische 1, wobei der Invertierer 539 das Signal des Datenbusses a(2 : 0) empfängt. Der Multiplexer 575 wählt den Ausgangswert PBSR des Speicherblockregisters 759 der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 aus. Während des Kennwortvergleichszyklus COMPCYCLE der Zeitablaufsteuersignalerzeugungsschaltung 405 erzeugt das NICHT-ODER-Gatter 507 eine logische 0, wobei durch die Ausgaben des ODER-Gatters 553 und der UND-Gatter 557, 559 und 561 vom jeweiligen Block nur der Kennwortaufzeichnungsbereich direkt zugewiesen wird. Wie in (9c) der Fig. 9 gezeigt, werden die im EEPROM 107 aufgezeichneten Kennwortdaten über den Datenbus ad(7 : 0) an das Exklusiv-ODER-Gatter 523 angelegt.

Wenn der Speicherblock zugewiesen ist und die Kennwortregisterauswahldecodierer 742 bis 752 nacheinander vom Datenbus a(7 : 0) ausgewählt werden, um die Kennwortaufzeichnungsregister 761 bis 773 freizugeben, werden die von der SIO 101 gesendeten Kennwortdaten über den Datenbus idb(7 : 0) der CPU 103 byteweise nacheinander aufgezeichnet. Das Adreßsignal des Datenbusses add(2 : 0) des Multiplexers 655 der Zeitablaufsteuersignalerzeugungsschaltung 405 liegt an den NICHT-UND-Gattern 775 bis 787 an, wobei die Invertierer 709 bis 721, die mit den Ausgängen der NICHT-UND-Gatter 775 bis 787 verbunden sind, die Kennwortaufzeichnungsregister 761 bis 773 freigeben, wodurch die Kennwortdaten erzeugt werden, wie in (9i) der Fig. 9 gezeigt ist. Die Werte der in (9i) der Fig. 9 und in (9c) der Fig. 9 gezeigten Kennwortdaten werden im Exklusiv-ODER-Gatter 523 verglichen. Wenn ein Kennwortvergleich für ein Byte abgeschlossen ist, wird das Vergleichsergebnis über das NICHT-UND-Gatter 502 im Flipflop 577 abgelegt. Dann wird der Kennwortvergleich für das nächste Datenbyte durchgeführt, wobei das Vergleichsergebnis im Flipflop 579 abgelegt wird.

Wenn der Vergleich für alle Kennwortbytes abgeschlossen ist und die Flipflops 579 bis 589 eine logische 1 erzeugen, erzeugt das UND-Gatter 505 eine logische 1, wie in (9n) der Fig. 9 gezeigt ist. Da der Ausgang des ODER-Gatters 547 eine logische 1 aufweist, wie in (9g) der Fig. 9 gezeigt ist, und der Ausgang des Flipflops 571 eine logische 0 aufweist, gibt das Flipflop 573 eine logische 1 aus, wie in (9w) der Fig. 9 gezeigt ist. Das Zugriffsteuersignal ACCESS mit einer logischen 1 liegt am NICHT-ODER-Gatter 615 der Zeitablaufsteuersignalerzeugungsschaltung 405 an, wobei das NICHT-ODER-Gatter 615 eine logische 0 ausgibt. Das Zugriffsteuersignal ACCESS liegt ferner am Dreistufenpuffer 727 der Informationsschutzüberprüfungszustandsignal-Erzeugungsschaltung 720 der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung 407 an. Die CPU 103 kann über den Bustreiber 702 den Betriebszustand überprüfen.

Wenn somit das Kennwort im Datenspeicherbereich des EEPROMs 107 mit dem von außen empfangenen Kennwort übereinstimmt, kann auf die Daten eines zugehörigen Blocks zugegriffen werden. Da auf die Daten anderer Blöcke nicht zugegriffen werden kann, ist die Zuverlässigkeit für eine Geheimhaltung verbessert.

Im folgenden wird der Kennwortvergleichsfehlermodus beschrieben. Ein Kennwortvergleichsfehlermodus bedeutet, daß es unmöglich ist, auf die Daten zuzugreifen, da das im Datenspeicherblock festgelegte Kennwort nicht mit dem von außen empfangenen Kennwort übereinstimmt. Für den Fall, daß das Kennwort nicht übereinstimmt, wie in (10c) und (10i) der Fig. 10 gezeigt ist, wird keine Beschreibung gegeben. Das Exklusiv-ODER-Gatter 523 vergleicht das Kennwort bitweise. Wenn der Kennwortvergleich für ein Byte abgeschlossen ist, wird das Vergleichsergebnis über das NICHT-

UND-Gatter 502 in das Flipflop 579 eingetragen.

Wenn wie in (10c) und (10i) der Fig. 10 gezeigt das Kennwort nicht übereinstimmt, erzeugen die Flipflops 587 und 589 eine logische 0, wobei der Ausgang des UND-Gatters 505 auf einer logischen 0 gehalten wird, wie in (10n) der Fig. 10 gezeigt ist. Da der Ausgang des Flipflops 573 der Zugriffsteuersignalerzeugungsschaltung 403 auf einer logischen 0 gehalten wird, wie in (10w) der Fig. 10 gezeigt ist, kann auf die Daten dieses Blocks nicht zugegriffen werden.

Wie oben beschrieben worden ist, wird der Kennwortvergleichsvorgang mittels Hardware verwirklicht, um die Belastung der CPU zu verringern und den Kennwortvergleichsvorgang komplizierter zu machen. Damit wird eine Geheimhaltung des Datenspeichers sichergestellt und die Zuverlässigkeit der Datenspeicherung verbessert.

Obwohl die Erfindung mit Bezug auf eine bevorzugte Ausführungsform derselben genau gezeigt und beschrieben worden ist, ist klar, daß Fachleute vorangegangene und andere Abwandlungen in Form und in Einzelheiten durchführen können, ohne den Umfang der Erfindung zu verlassen.

Patentansprüche

1. Intelligente Karte, **gekennzeichnet durch**
einen Datenspeicher (107), der in n Blöcke aufgeteilt ist, wobei ein Statuswert anzeigt, ob ein Kennwort vorhanden ist, wobei das Kennwort im Vorspann jedes Blocks des Datenspeichers (107) aufgezeichnet ist;
eine Steuervorrichtung zum Erzeugen von Signalen bezüglich der Aufteilung des Datenspeichers (107) und zum Bereitstellen von Kennwortdaten; und
eine Informationsschutzvorrichtung zum Durchsuchen eines abgeteilten Speicherbereichs und zum Zugreifen auf Speicherinformation des Speicherbereiches, wenn das im abgeteilten Datenspeicherbereich aufgezeichnete Kennwort mit dem von außen eingegebenen Kennwort übereinstimmt.

2. Verfahren zum Zugreifen auf einen Datenspeicher (107) einer intelligenten Karte, gekennzeichnet durch die Schritte:
Aufteilen des Datenspeichers in n Blöcke;
Aufzeichnen eines Statuswertes, der anzeigt, ob ein Kennwort vorhanden ist, und des Kennworts an der gleichen Position in jedem Block des Datenspeichers (107) liegt;
Vergleichen des im jeweiligen Block aufgezeichneten Kennwortes mit einem von außen empfangenen Kennwort; und
Zugreifen auf einen Informationsspeicherbereich, wenn die Kennworte übereinstimmen.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß der Datenspeicher in Blöcke mit konstanter Größe aufgeteilt ist, wobei der Statuswert und das Kennwort im Vorspann jedes Blocks aufgezeichnet werden.

4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß die abgeteilten Blöcke die gleiche Größe besitzen oder sich in Abhängigkeit von den Eigenschaften der Speicherinformation in ihrer Größe unterscheiden.

5. Intelligente Karte, gekennzeichnet durch
einen Datenspeicher (107) zum Speichern eines Betriebsprogramms der intelligenten Karte und von Benutzerinformation;
einen Informationsschutzprozessor (201) zum Schützen eines Benutzerinformationsspeicherbereiches des Datenspeichers (107); und
eine Steuervorrichtung zum direkten Zugreifen auf einen Betriebsprogrammspeicherbereich oder den Informationsschutzprozessor (201), der ein Kennwort erfordert, so daß der Benutzerinformationsspeicherbereich nicht willkürlich verwendet werden kann, und zum Zugreifen auf den Benutzerinformationsspeicherbereich über einen Kennwortvergleichsvorgang des Informationsschutzprozessors (201).

6. Intelligente Karte nach Anspruch 5, dadurch gekennzeichnet, daß der Informationsschutzprozessor (201) enthält:
eine Speicheraufteilungs- und Kennwortdatenempfangsschaltung (407), die ein Zuweisungssignal erzeugt, auf einen Kennwortspeicherbereich des jeweiligen Blocks zugreift und ein von außen empfangenes Kennwort empfängt;
eine Kennwortvergleichsschaltung (409, 419, 421) zum Vergleichen des von der Speicheraufteilungs- und Kennwortdatenempfangsschaltung (407) bereitgestellten Kennwortes mit dem im Datenspeicher (107) gespeicherten Kennwort;
eine Zugriffsteuersignalerzeugungsschaltung (403) zum Erzeugen eines Zugriffsteuersignals, die auf den Datenspeicher (107) zugreift, wenn beide Kennwörter übereinstimmen;
eine Kennwortaufzeichnungsbereichfestlegungsschaltung (415) zum bevorzugten Zuweisen eines Kennwortaufzeichnungsbereiches, wenn ein bezeichneter Block des Datenspeichers (107) ausgewählt ist, und zum Festlegen eines Informationsaufzeichnungsbereiches, auf den zugegriffen werden soll;
eine Zugriffadressenerzeugungsschaltung (413) zum Erzeugen eines Adreßsignals für den Kennwort- und Informationszugriff aus den Ausgaben der Speicheraufteilungs- und Kennwortdatenempfangsschaltung (407) und der Kennwortaufzeichnungsbereichfestlegungsschaltung (415); und
eine Zeitablaufsteuersignalerzeugungsschaltung (405) zum Erzeugen eines Adreßsignals, die einen Block für den Zugriff auf den Datenspeicher (107) zuweist und ein Zeitablaufsteuersignal für einen Kennwortvergleich erzeugt.

7. Intelligente Karte nach Anspruch 6, dadurch gekennzeichnet, daß die Kennwortvergleichsschaltung (409, 419, 421) enthält:
einen ersten Kennwortkomparator (419) zum bitweisen Vergleichen eines Kennwortbytes;
eine Vergleichsergebniszwischenspeicherschaltung (409) zum Speichern der Ausgabe des ersten Kennwortkomparators (419); und
einen zweiten Kennwortkomparator (421) zum Bestätigen der Vergleichsergebnisse für alle Bytes.

8. Intelligente Karte mit einer seriellen Eingabe/Ausgabe-Vorrichtung (SIO), einer Zentraleinheit (CPU) sowie einem elektrisch löschbaren und programmierbaren Nur-Lese-Speicher (EEPROM), gekennzeichnet durch einen Informationsschutzprozessor (201), der mit den Daten-, Adreß- und Steuerbussen der CPU und den Daten-, Adreß- und Steuerbussen des EEPROMs verbunden ist, um einen Datenspeicher des EEPROMs vor einem Zugriff zu schützen.

9. Intelligente Karte nach Anspruch 8, dadurch gekennzeichnet, daß der Informationsschutzprozessor (201) enthält:
eine Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung (407) zum Decodieren des Datenspeicherblockauswahl- und Kennworterzeugungsadreßauswahlsignals, das von der CPU erzeugt wird, um Daten zum Auswählen eines abgeteilten Blocks des Datenspeichers (107) und einen Kennwortaufzeichnungsbereich zu erzeugen, der die von außen empfangenen Kennwortdaten aufzeichnet, um die Kennwortdaten zum Vergleichszeitpunkt zu erzeugen, wobei in Abhängigkeit von einem Lesesteuersignal der CPU ein Datenspeicherzugriffssignal oder ein Vergleichsverarbeitungszustandssignal ausgegeben wird und die vom Kennwortvergleichsvorgang erzeugten Kennwortdaten ausgegeben werden;
einen ersten Kennwortkomparator (419) zum bitweisen Vergleichen der von der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung (407) erzeugten Kennwortdaten mit dem in einem ausgewählten Bereich des Datenspeichers (107) aufgezeichneten Kennwort, um ein Kennwortvergleichsergebnis für ein Byte zu erzeugen;
eine Kennwortzwischenspeicherschaltung (409) zum Zwischenspeichern des Kennwortvergleichsergebnisses, bis ein Kennwortvergleich für alle Bytes abgeschlossen ist;
einen zweiten Kennwortkomparator (421) zum erneuten Bestätigen des Kennwortvergleichsergebnisses für alle Bytes, die in der Kennwortzwischenspeicherschaltung (409) gespeichert sind, vor dem Vergleichsabschlußzeitpunkt;
eine Zugriffsteuersignalerzeugungsschaltung (403) zum Erzeugen eines Zugriffsteuersignals, das anzeigt, daß auf einen ausgewählten Bereich des Datenspeichers (107) zugegriffen werden kann, wenn das vom zweiten Kennwortkomparator (421) erzeugte Kennwortvergleichsergebnis positiv ist und eine Information vorliegt, die anzeigt, daß im ausgewählten Bereich des Datenspeichers (107) ein Kennwort vorliegt;
eine Zeitablaufsteuersignalerzeugungsschaltung (405) zum Zählen eines Taktes in Abhängigkeit von einem Startsignal, das gleichzeitig mit der Blockzuweisungsdecodierung der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung (407) erzeugt wird, um ein Decodierungssignal für das Lesen eines Kennwortvergleichszyklus, ein Vergleichstaktsignal und das in der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung (407) aufgezeichnete Kennwort zu erzeugen, wobei ein Kennwortvergleichsabschlußsteuersignal an den zweiten Kennwortkomparator (421) angelegt wird;
eine Kennwortspeicherbereichfestlegungsschaltung (415) zum Erzeugen einer Adresse zum bevorzugten Zuweisen des Kennwortaufzeichnungsbereichs jedes Blocks des Datenspeichers (107); und
eine Zugriffadreßsignalerzeugungsschaltung (413) zum Auswählen eines Blocks des in N Blöcke aufgeteilten Datenspeichers (107) mittels eines Signals, das von der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung (407) erzeugt wird, die ein Adreßsignal zum Zuweisen eines Kennwortzugriffsbereiches erzeugt und ein Adreßsignal zum Zugreifen auf einen Informationsspeicherbereich erzeugt, wenn ein Kennwortvergleich abgeschlossen ist.

10. Intelligente Karte nach Anspruch 9, dadurch gekennzeichnet, daß die Zeitablaufsteuersignalerzeugungsschaltung (405) enthält:
einen Zähler zum Zählen eines Kennwortvergleichstaktes; eine Auswahlschaltung zum Auswählen eines Adreßsignals, das in Abhängigkeit vom Kennwortvergleichstakt des Zählers vom Zähler oder der CPU erzeugt wird, um das Kennwort zu erzeugen;
eine Vergleichstakterzeugungsschaltung zum Erzeugen eines Vergleichstaktes, der in Abhängigkeit von der Ausgabe des Zählers während eines Kennwortvergleiches benötigt wird; und
eine Vergleichsabschlußsignalerzeugungsschaltung zum Erzeugen eines Vergleichsabschlußsignals aus der Ausgabe des Zählers.

11. Intelligente Karte nach Anspruch 9, dadurch gekennzeichnet, daß die Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung (407) enthält:
einen Blockauswahlregisteradreßdecodierer zum Erzeugen eines Decodierungssignals zum Auswählen eines Blocks des Datenspeichers (107) und zum Erzeugen eines Startsignals;
einen Kennwortregisteradreßdecodierer zum Decodieren eines Adreßsignals, um eine Kennwortaufzeichnungsadresse innerhalb des jeweiligen Blocks des Datenspeichers (107) auszuwählen;
ein Blockaufteilungsregister zum Speichern eines Blockaufteilungssignals gemäß der Ausgabe des Blockauswahlregisteradreßdecodierers;
ein Kennwortregister zum Speichern eines von außen angelegten Kennwortes in Abhängigkeit von der Ausgabe des Kennwortregisteradreßdecodierers;
ein Statuswertregister zum Speichern eines Statuswertes gemäß dem Informationsschutz des Datenspeichers;
einen Statuswertlesedecodierer zum Auslesen des Statuswertes;
einen Treiber zum Steuern des Statuswertes, der aufgrund der Ausgabe des Statuswertlesedecodierers von der CPU gelesen werden soll; und
eine Registerlesesteuervorrichtung zum Erzeugen eines Torsignals, so daß das Kennwort und ein Wert des Blockaufteilungsregisters gelesen werden.

12. Intelligente Karte nach Anspruch 9, dadurch gekennzeichnet, daß der erste Kennwortkomparator (419) enthält:
ein Exklusiv-ODER-Gatter (523) zum bitweisen Vergleichen des vom Datenspeicher (107) erzeugten Kennwortes mit dem von der Speicherblockauswahlsignalerzeugungs- und Kennwortdatenempfangsschaltung (407) erzeugten Kennwort; und
ein NICHT-UND-Gatter (502) zum Erzeugen eines Kennwortvergleichsergebnisses für ein Byte.

13. Intelligente Karte nach Anspruch 9, dadurch gekennzeichnet, daß die Kennwortzwischenspeicherschaltung (409) enthält:
ein NICHT-ODER-Gatter (525) mit Eingangsanschlüssen, die mit einem Rücksetzsignal und mit dem Startsignal verbunden sind; und
mehrere Flipflops (579—589) mit entsprechenden mit einem Kennwortvergleichstaktsignal der Zeit-

ablaufsteuersignalerzeugungsschaltung (405) verbundenen Taktanschlüssen, wobei die Flipflops (579—589) jeweils Rücksetzanschlüsse besitzen, die mit dem Ausgang des NICHT-ODER-Gatters (525) verbunden sind, und jeweils Ausgangsanschlüsse besitzen, die mit dem zweiten Kennwortkomparator (421) verbunden sind.

Hierzu 9 Seite(n) Zeichnungen

– Leerseite –

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

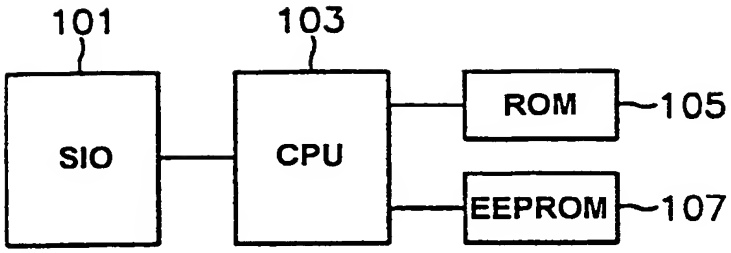

FIG. 1

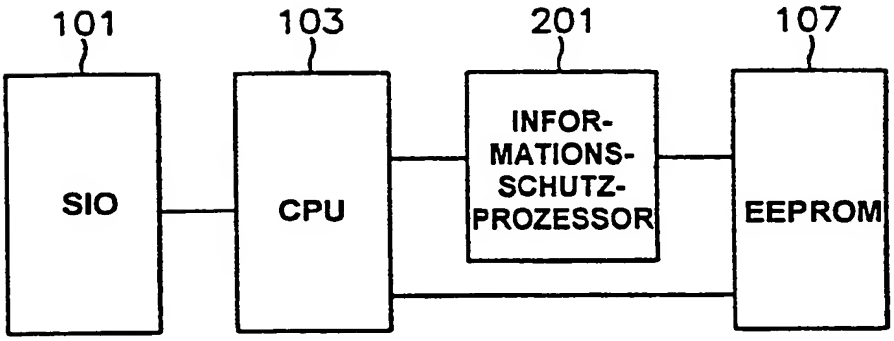

FIG. 2

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

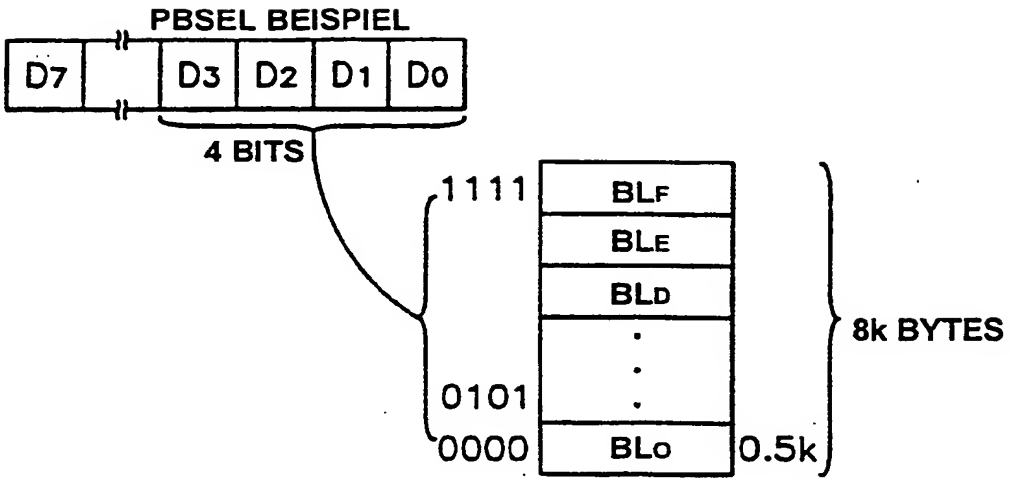

FIG. 3A

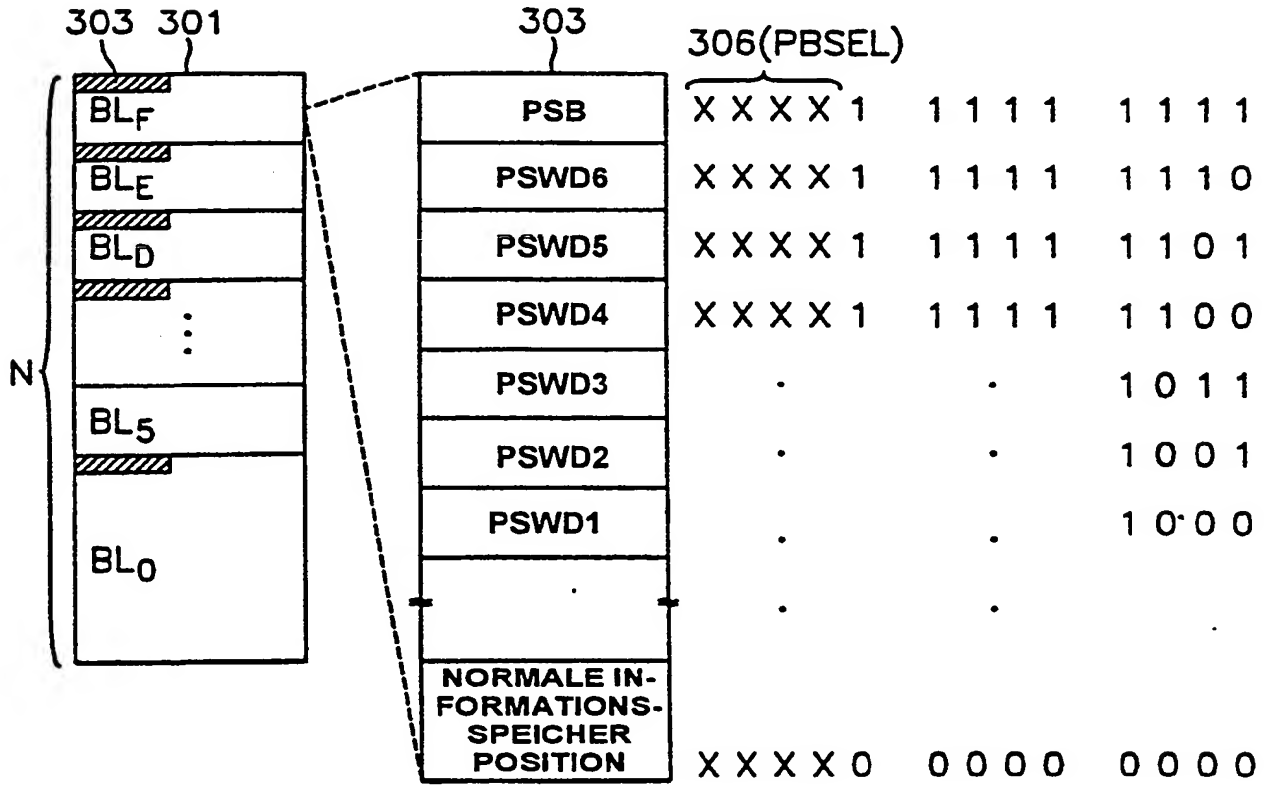

FIG. 3B

602 014/506

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

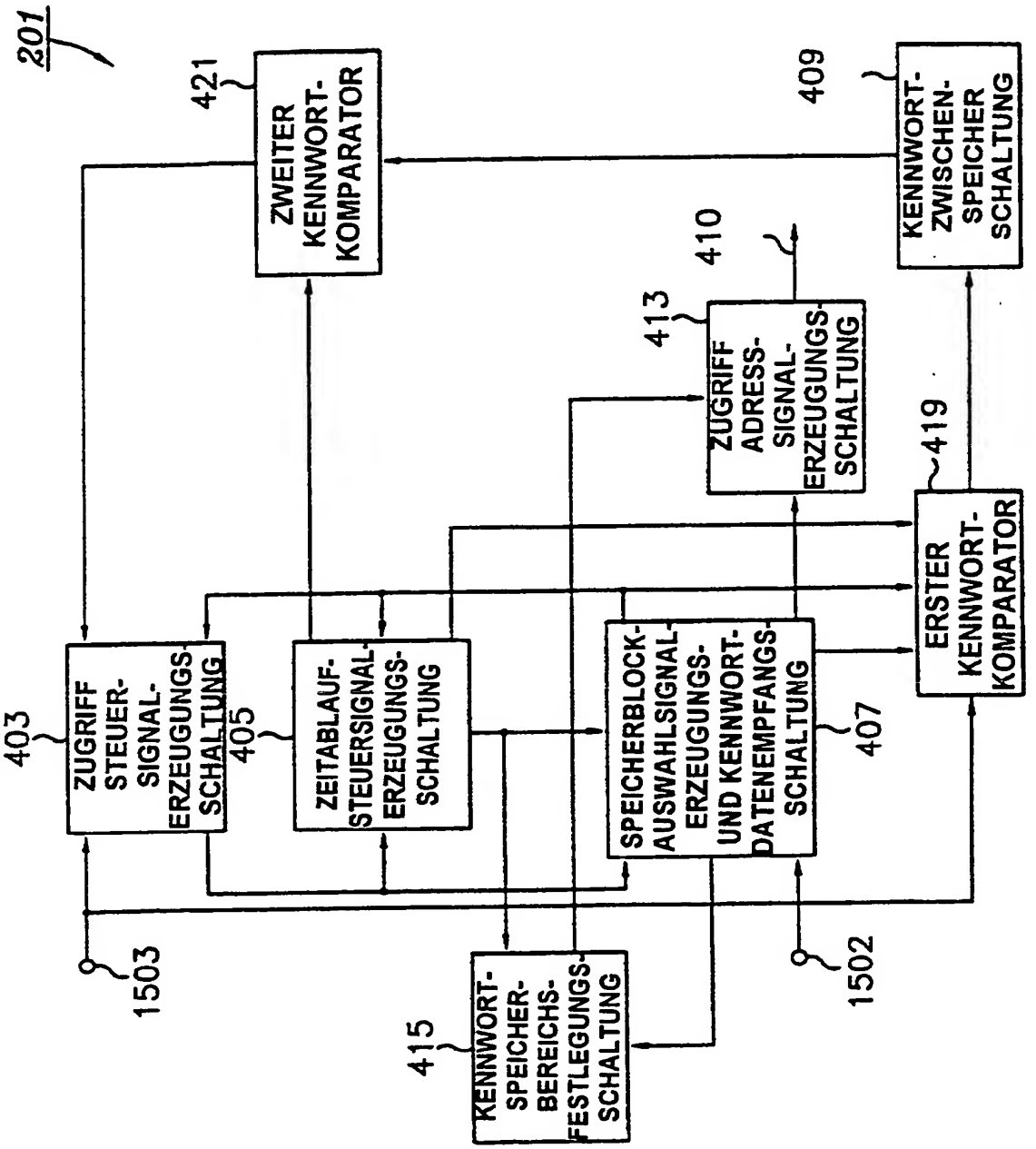

FIG. 4

602 014/506

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

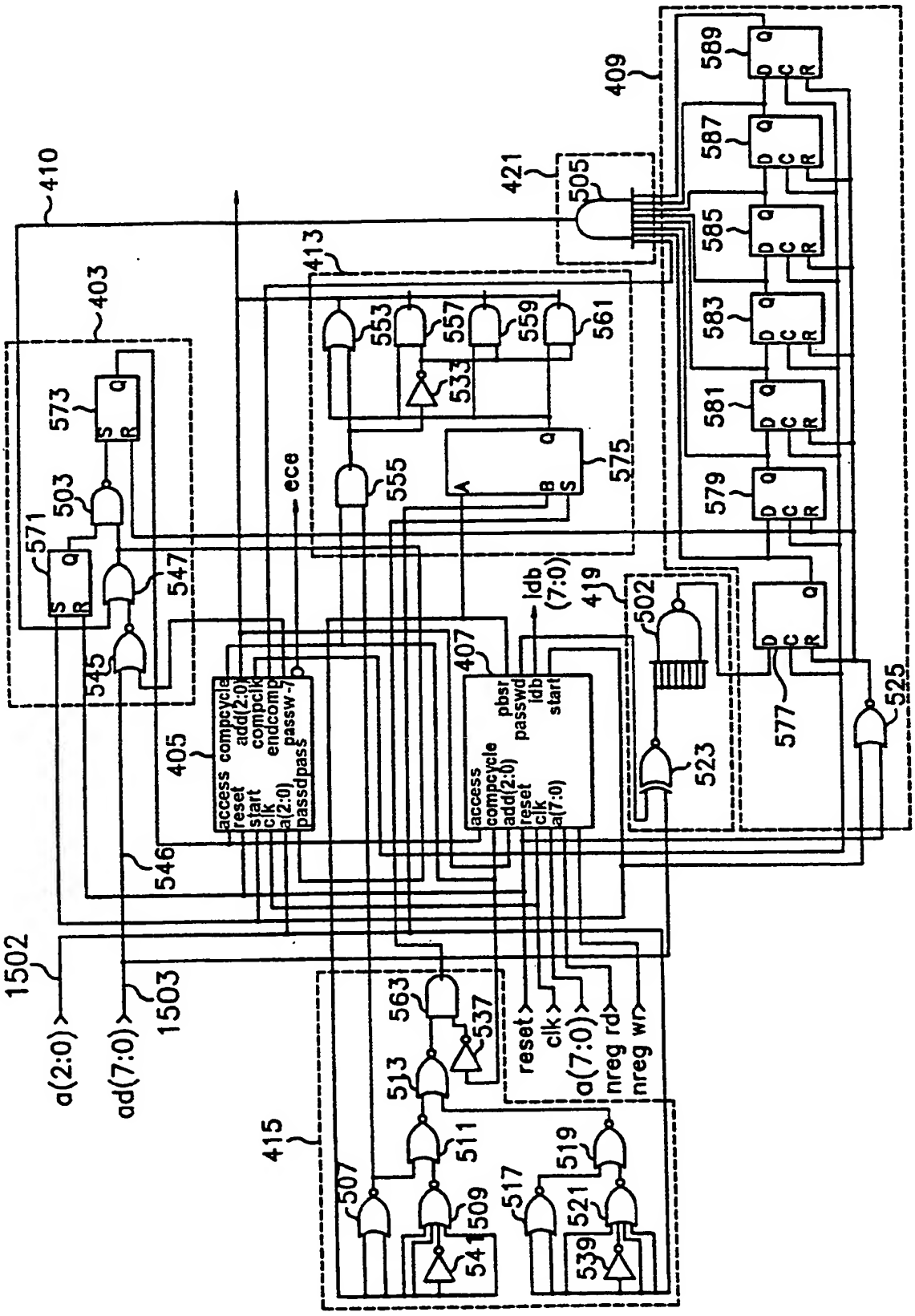

FIG. 5

602 014/506

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

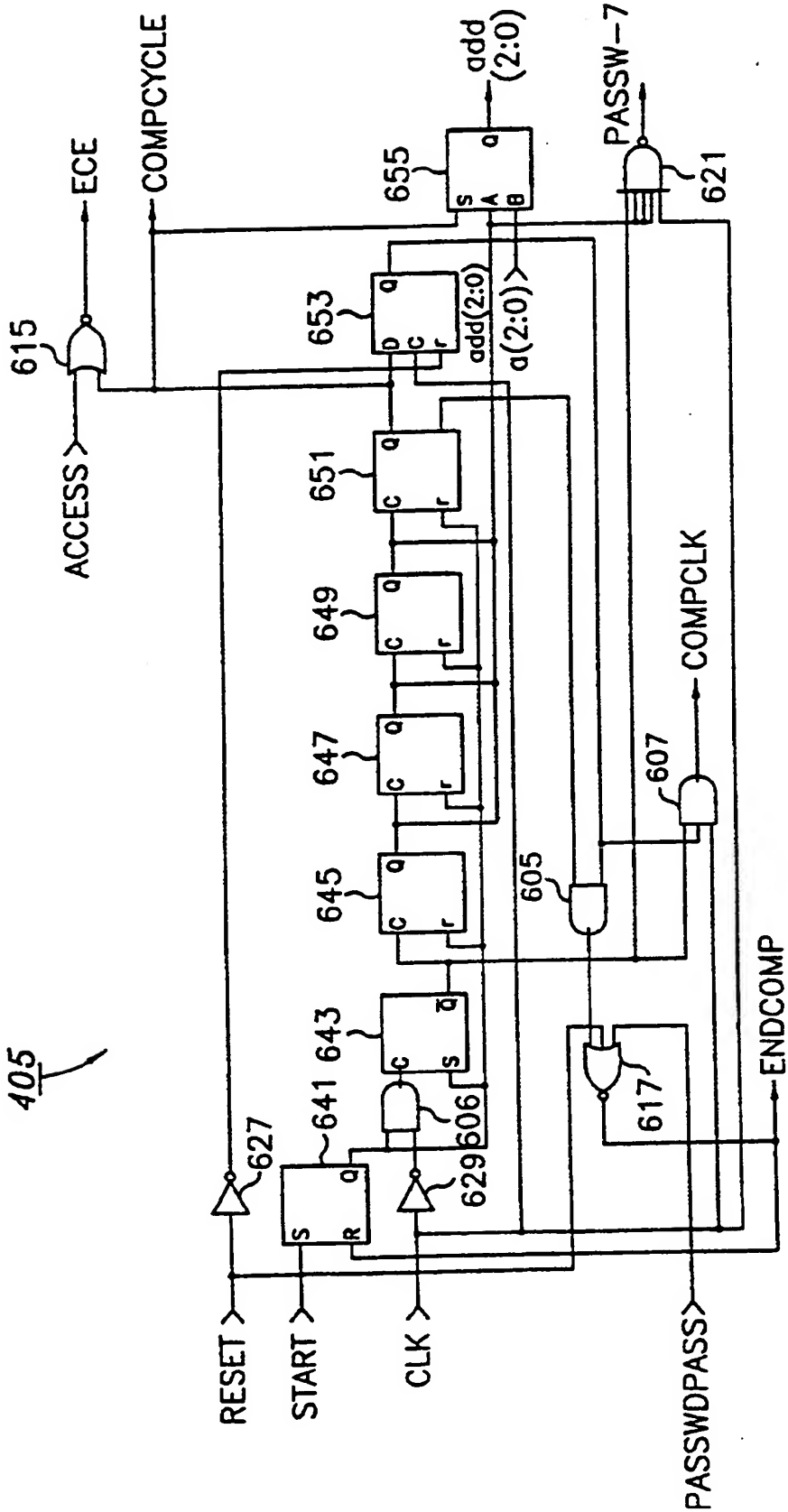

FIG. 6

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

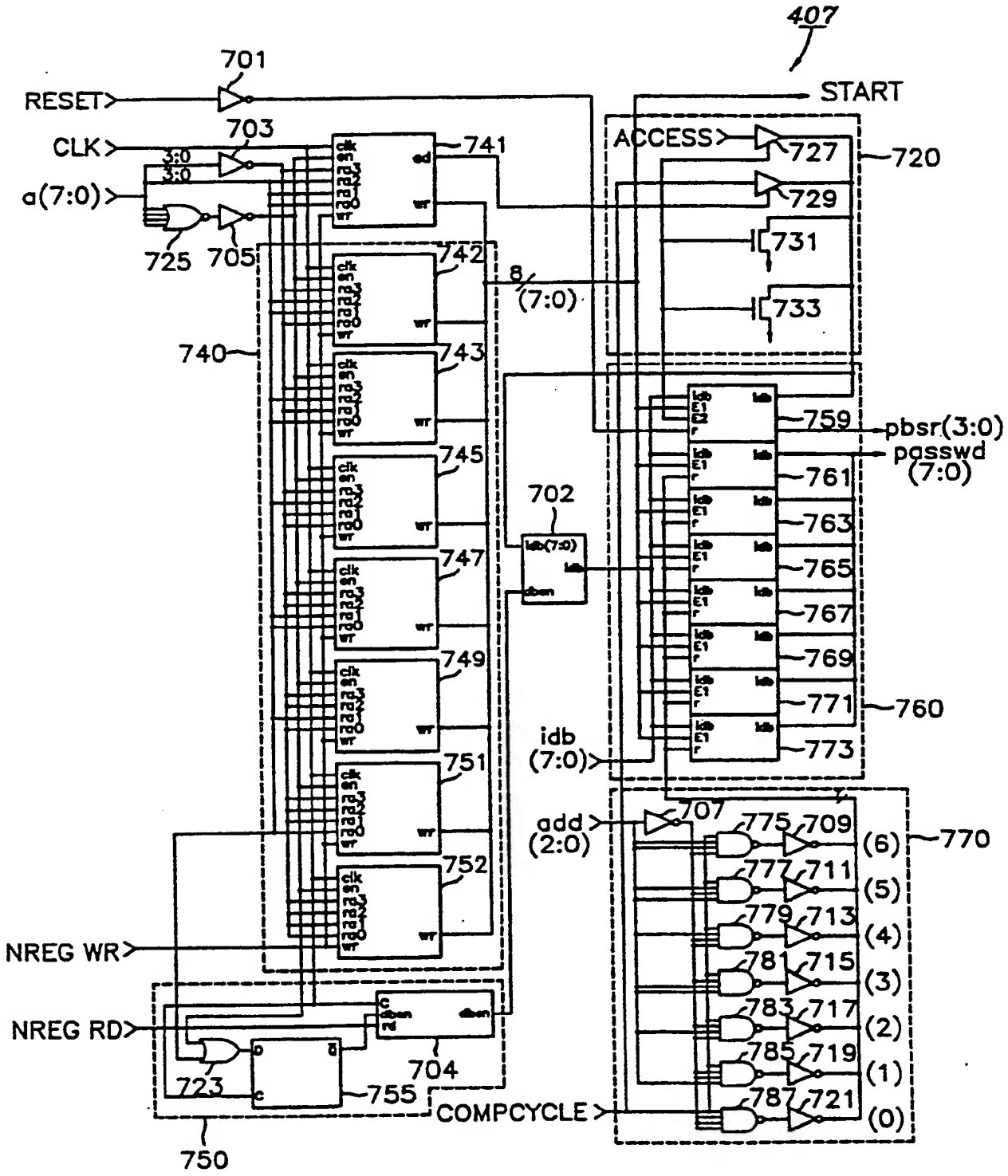

FIG. 7

602 014/506

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

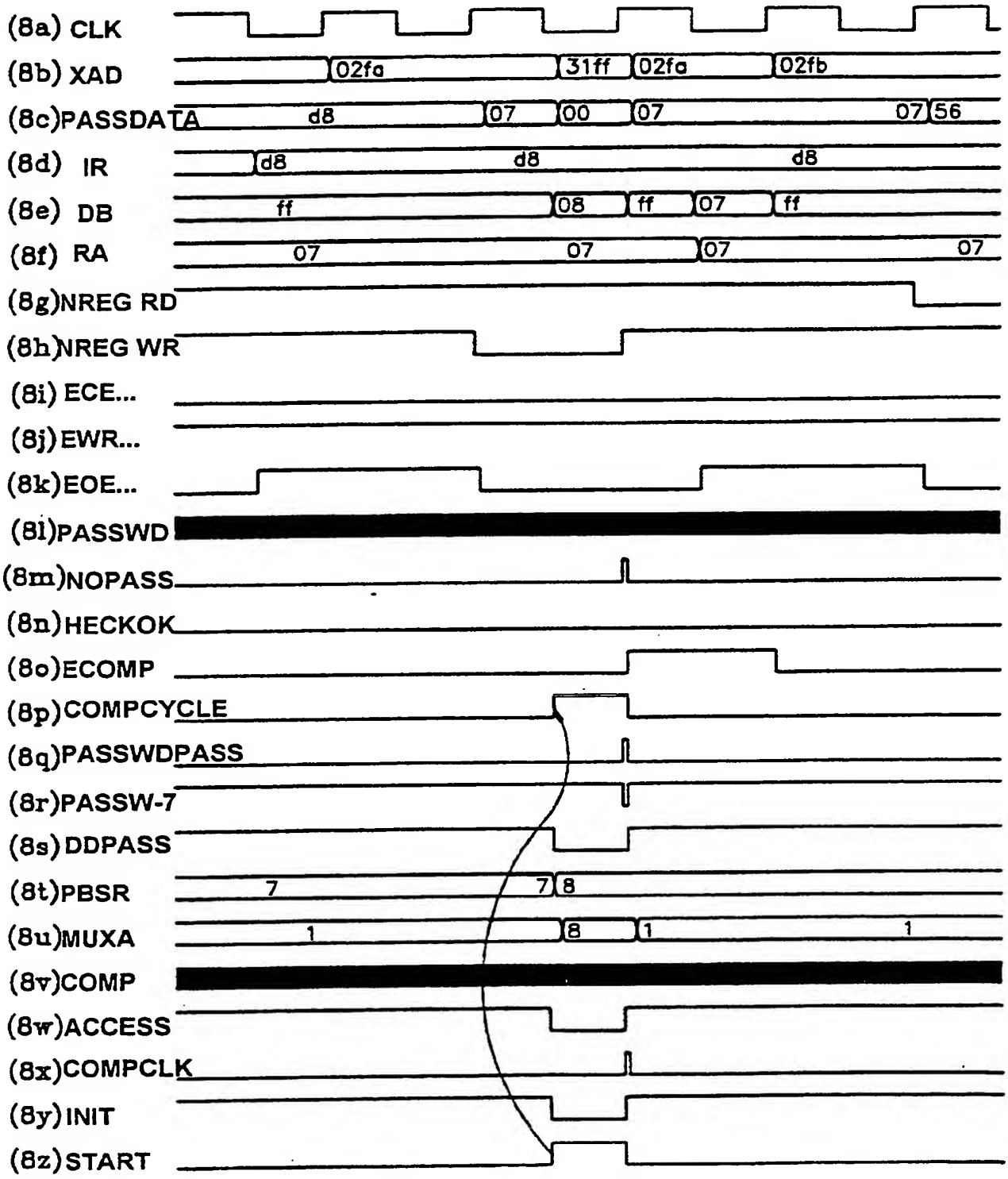

FIG. 8

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

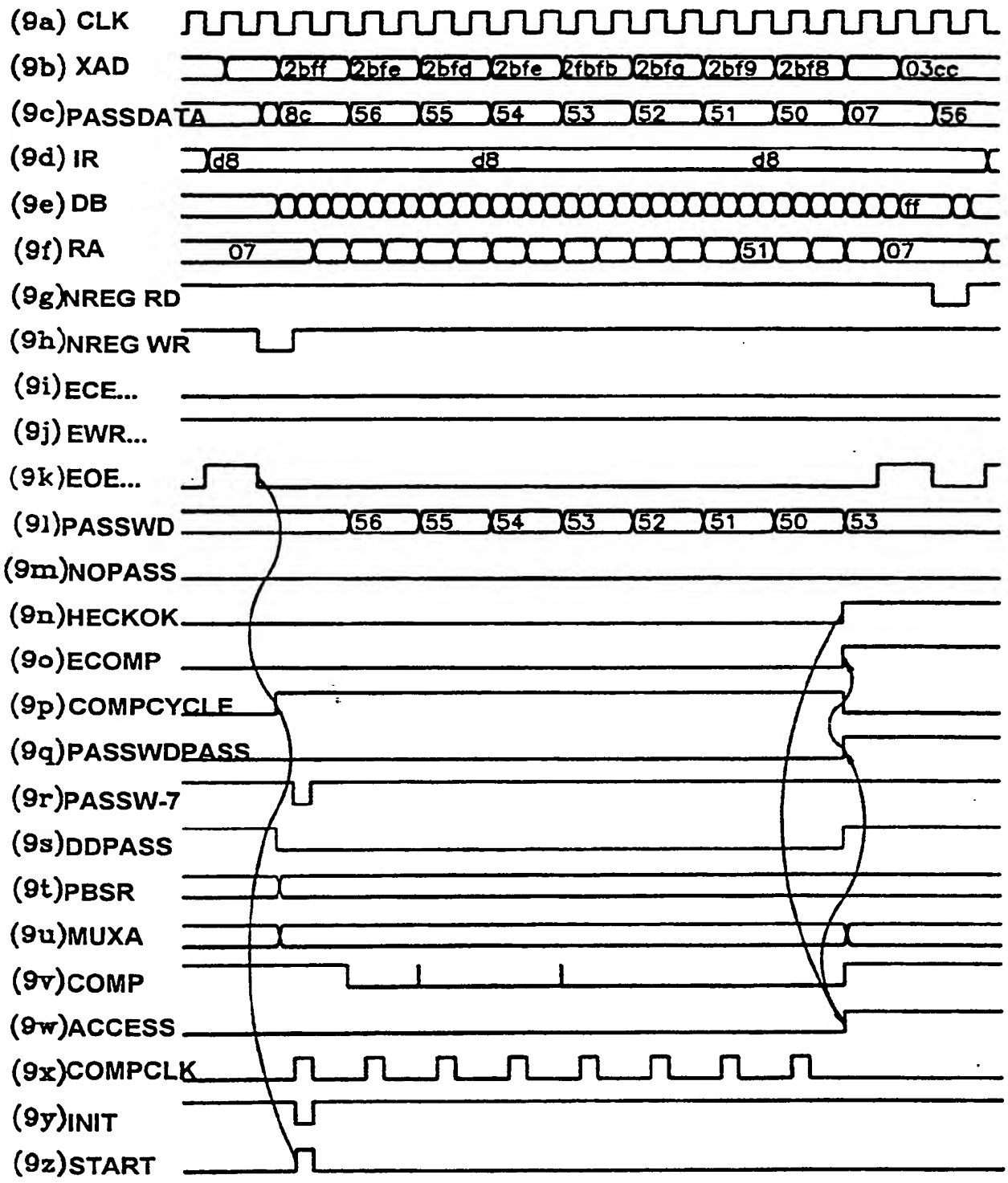

FIG. 9

Nummer: DE 195 36 206 A1
Int. Cl.[6]: G 06 K 19/073
Offenlegungstag: 4. April 1996

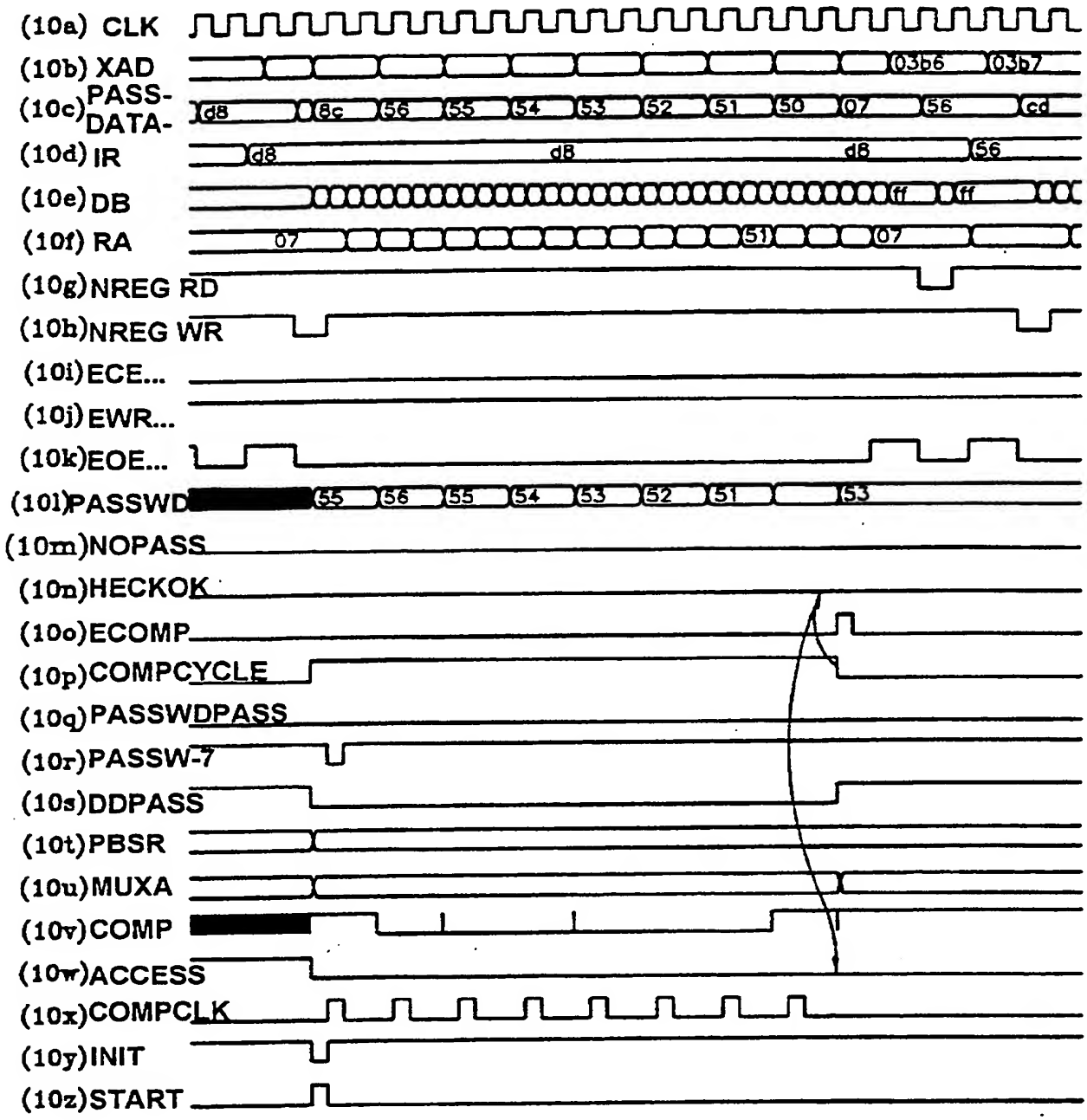

FIG. 10